AMENDMENTS TO THE CLAIMS

Claims Pending:

- At time of the Action: Claims 1-72
- Allowable Subject Matter: Claim 5-15, 19-26, 30-37, 43-46, 49, 52, 53-55, 58-63, 67-68, and 71-72
- Amended Claims: Claims 1, 4, 6-8, 11, 14, 16, 20, 26, 27, 31-34, 37, 38, 40-41, 44, 47, 50, 53-56, 65, and 69
- Cancelled Claims: Claims 2, 3, 5, 17-19, 29, 30, 39, 43, 48-49, 51-52, 58, 67, and 71
- After this Response: Claims 1, 4, 6-16, 20-28, 31-38, 40-42, 44-50, 53-57, 59-66, 68-70, and 72

This listing of claims will replace all prior versions and listings, of claims in the application.

1. (Currently Amended) A method comprising:

selecting an elliptic curve;

determining a Squared Weil pairing based on ~~said~~ the elliptic curve, wherein the elliptic curve includes an elliptic curve E over a field K, wherein E can be represented as an equation $y^2 = x^3 + ax + b$; ~~and~~

wherein determining the Squared Weil pairing based on the elliptic curve further includes establishing a point id that is defined as a point at infinity on E, and wherein P, Q, R, X are points on E wherein X is an indeterminate denoting an independent variable of a function, and wherein $x(X)$, $y(X)$ are functions mapping the point X on E to its affine x and y coordinates, and wherein a line passes through the points P, Q, R if $P + Q + R = \text{id}$;

wherein determining the Squared Weil pairing based on the elliptic curve further includes:

with a first function $f_{j,P}$ and a second function $f_{k,P}$ for two integers j and k, deriving a third function $f_{-j-k,P}$ based on the first and second functions;

cryptographically processing selected information based on ~~said~~ the Squared Weil pairing;

outputting validation of selected information based on the Squared Weir pairing; and

determining a course of action in response to validation of selected information.

2.-3. (Cancelled).

4. (Currently Amended) The method as recited in Claim ~~3~~ 1, wherein when at least two of said P, Q, R points are equal, said line is a tangent line at a common point.

5. (Cancelled).

6. (Currently Amended) The method as recited in Claim ~~5~~ 1, wherein $(f_{-j-k,P}\, f_{j,P}\, f_{k,P}) = (f_{-j-k,\,P}) + (f_{j,\,P}) + (f_{k,\,P}) = 3(\mathrm{id}) - ((-j-k)P) - (jP) - (kP)$.

7. (Currently Amended) The method as recited in Claim ~~5~~ 1, wherein $f_{-j-k,P}(X)\ f_{j,P}(X)\ f_{k,P}(X)\ \mathrm{line}(jP, kP, (-j-k)P)(X) =$ a constant.

8. (Currently Amended) The method as recited in Claim ~~5~~ 1, wherein if j is an integer and P a point on E, then said first and second functions are rational functions on E whose divisor of zeros and poles is $(f_{j,P}) = j(P) - (jP) - (j-1)(\mathrm{id})$.

9. (Original) The method as recited in Claim 8, wherein if $j > 1$ and P, jP, and id are distinct, then said first function has a j-fold zero at $X = P$, a simple pole at $X = jP$, a $(j-1)$-fold pole at infinity, and no other poles or zeros.

10. (Original) The method as recited in Claim 8, wherein if j equals 0 or 1 then said first function is a nonzero constant.

11. (Currently Amended) The method as recited in Claim ~~5~~ 1,, further comprising determining $f_{0,P}$ such that a line through $0P$ = id, $(-j-k)P$, and $(j+k)P$ is vertical in that its equation does not reference a y-coordinate.

12. (Original) The method as recited in Claim 11, wherein:

$$f_{j+k,\boldsymbol{P}}(\boldsymbol{X}) = f_{j,\boldsymbol{P}}(\boldsymbol{X}) f_{k,\boldsymbol{P}}(\boldsymbol{X}) \frac{\mathrm{line}\left(j\boldsymbol{P}, k\boldsymbol{P}, (-j-k)\boldsymbol{P}\right)(\boldsymbol{X})}{\mathrm{line}\left(\boldsymbol{id}, (-j-k)\boldsymbol{P}, (j+k)\boldsymbol{P}\right)(\boldsymbol{X})}, \text{ and}$$

$$f_{j-k,\boldsymbol{P}}(\boldsymbol{X}) = \frac{f_{j,\boldsymbol{P}}(\boldsymbol{X})\mathrm{line}\left(\boldsymbol{id}, j\boldsymbol{P}, -j\boldsymbol{P}\right)(\boldsymbol{X})}{f_{k,\boldsymbol{P}}(\boldsymbol{X})\mathrm{line}\left(-j\boldsymbol{P}, k\boldsymbol{P}, (j-k)\boldsymbol{P}\right)(\boldsymbol{X})}.$$

13. (Original) The method as recited in Claim 11, wherein:

$f_{j,\,id}$ = constant;

$f_{j,-P}(X) = f_{j,P}(-X)$*(constant); and

if $(P+Q+R = \mathrm{id})$, then:

$$f_{j,\boldsymbol{P}}(\boldsymbol{X}) f_{j,\boldsymbol{Q}}(\boldsymbol{X}) f_{j,\boldsymbol{R}}(\boldsymbol{X}) = \frac{\mathrm{line}(\boldsymbol{P}, \boldsymbol{Q}, \boldsymbol{R})(\boldsymbol{X})^j}{\mathrm{line}(j\boldsymbol{P}, j\boldsymbol{Q}, j\boldsymbol{R})(\boldsymbol{X})}.$$

14. (Currently Amended) The method as recited in Claim ~~3~~ 1,, wherein P and Q are m-torsion points on E and m is an odd prime, and wherein determining said Squared Weil pairing further includes:

determining said squared Weil pairing based on

$$\frac{f_{m,\boldsymbol{P}}(\boldsymbol{Q})f_{m,\boldsymbol{Q}}(\boldsymbol{-P})}{f_{m,\boldsymbol{P}}(\boldsymbol{-Q})f_{m,\boldsymbol{Q}}(\boldsymbol{P})}=-e_m(\boldsymbol{P},\boldsymbol{Q})^2,$$

where e_m denotes the Weil-pairing.

15. (Original) The method as recited in Claim 14, wherein neither P nor Q is an identity and P is not equal to $\pm Q$.

16. (Currently Amended) A computer-readable medium having computer-implementable instructions for causing at least one processing unit to perform acts comprising:

determining a Squared Weil pairing based on an elliptic curve, wherein said elliptic curve includes an elliptic curve E over a field K, wherein E can be represented as an equation $y^2 = x^3 + ax + b$; ~~and~~

determining the Squared Weil pairing based on the elliptic curve further includes establishing a point id that is defined as a point at infinity on E, and wherein P, Q, R, X are points on E wherein X is an indeterminate denoting an independent variable of a function, and wherein $x(X)$, $y(X)$ are functions mapping said point X on E to its affine x and y coordinates, and wherein a line passes through said points P, Q, R if $P + Q + R = \text{id}$;

wherein determining the Squared Weil pairing based on the elliptic curve further includes:

determining a first function $f_{j,P}$ and a second function $f_{k,P}$ for two integers j and k; and

determining a third function $f_{-j-k,P}$ based on the first and second functions

cryptographically processing selected information based on ~~said~~ the Squared Weil pairing;

outputting validation of selected information based on the Squared Weil pairing and determining a course of action in response to the validation of selected information.

17.-19. (Cancelled).

20. (Currently Amended) The computer-readable medium as recited in Claim ~~19~~ 16, wherein $(f_{-j-k,P}\ f_{j,P}\ f_{k,P}) = (f_{-j-k,P}) + (f_{j,P}) + (f_{k,P}) = 3(\mathrm{id}) - ((-j-k)P) - (jP) - (kP)$.

21. (Original) The computer-readable medium as recited in Claim 20, wherein $f_{-j-k,P}(X)\ f_{j,P}(X)\ f_{k,P}(X)\ \mathrm{line}(jP, kP, (-j-k)P)(X) =$ a constant.

22. (Original) The computer-readable medium as recited in Claim 20, wherein if j is an integer and P a point on E, then said first and second functions *are* rational functions on E whose divisor of zeros and poles is $(f_{j,P}) = j(P) - (jP) - (j-1)(\mathrm{id})$.

23. (Original) The computer-readable medium as recited in Claim 20, further comprising determining $f_{0,P}$ such that a line through $0P = \mathrm{id}$, $(-j-k)P$, and $(j+k)P$ is vertical in that it does not reference a y-coordinate.

24. (Original) The computer-readable medium as recited in Claim 23, wherein:

$$f_{j+k,\boldsymbol{P}}(\boldsymbol{X}) = f_{j,\boldsymbol{P}}(\boldsymbol{X}) f_{k,\boldsymbol{P}}(\boldsymbol{X}) \frac{\text{line}\left(j\boldsymbol{P}, k\boldsymbol{P}, (-j-k)\boldsymbol{P}\right)(\boldsymbol{X})}{\text{line}\left(\boldsymbol{id}, (-j-k)\boldsymbol{P}, (j+k)\boldsymbol{P}\right)(\boldsymbol{X})}, \text{ and}$$

$$f_{j-k,\boldsymbol{P}}(\boldsymbol{X}) = \frac{f_{j,\boldsymbol{P}}(\boldsymbol{X})\text{line}\left(\boldsymbol{id}, j\boldsymbol{P}, -j\boldsymbol{P}\right)(\boldsymbol{X})}{f_{k,\boldsymbol{P}}(\boldsymbol{X})\text{line}\left(-j\boldsymbol{P}, k\boldsymbol{P}, (j-k)\boldsymbol{P}\right)(\boldsymbol{X})}.$$

25. (Original) The computer-readable medium as recited in Claim 23, wherein:

$f_{j,\text{id}}$ = constant;

$f_{j,-P}(X) = f_{j,P}(-X)$*(constant); and

if ($P + Q + R = \text{id}$), then:

$$f_{j,\boldsymbol{P}}(\boldsymbol{X}) f_{j,\boldsymbol{Q}}(\boldsymbol{X}) f_{j,\boldsymbol{R}}(\boldsymbol{X}) = \frac{\text{line}(\boldsymbol{P}, \boldsymbol{Q}, \boldsymbol{R})(\boldsymbol{X})^j}{\text{line}(j\boldsymbol{P}, j\boldsymbol{Q}, j\boldsymbol{R})(\boldsymbol{X})}.$$

26. (Currently Amended) The computer-readable medium as recited in Claim ~~18~~ 16, wherein P and Q are m-torsion points on E and m is an odd prime, and wherein determining said Squared Weil pairing further includes:

determining said squared Weil pairing based on

$$\frac{f_{m,\boldsymbol{P}}(\boldsymbol{Q}) f_{m,\boldsymbol{Q}}(-\boldsymbol{P})}{f_{m,\boldsymbol{P}}(-\boldsymbol{Q}) f_{m,\boldsymbol{Q}}(\boldsymbol{P})} = -e_m(\boldsymbol{P}, \boldsymbol{Q})^2,$$

where e_m denotes the Weil-pairing.

27. (Currently Amended) An apparatus comprising:

memory configured to store information suitable for use with using a cryptographic process;

a logic operatively coupled to ~~said~~ the memory and configured to determine a Squared Weil pairing based on at least one elliptic curve;

wherein the logic is further configured to establishing a point id that is defined as a point at infinity on E, and wherein P, Q, R, X are points on E wherein X is an indeterminate denoting an independent variable of a function, and wherein $x(X)$, $y(X)$ are functions mapping the point X on E to its affine x and y coordinates, and wherein a line passes through the points P, Q, R if $P + Q + R = \text{id}$;

wherein the logic is further configured to determine a first function $f_{j,P}$ and a second function $f_{k,P}$ for two integers j and k, and a third function $f_{-j-k,P}$ based on the first and second functions;

cryptographically process selected information stored in ~~said~~ the memory based on ~~said~~ the Squared Weil pairing;

a display device coupled to the logic for outputting validation of selected information; and

the logic determining a course of action in response to validation.

28. (Original) The apparatus as recited in Claim 27, wherein said logic is further configured to determine an elliptic curve E over a field K, wherein E can be represented as an equation $y^2 = x^3 + ax + b$.

29.-30. (Cancelled).

31. (Currently Amended) The apparatus as recited in Claim ~~30~~ 27, wherein $(f_{-j-k,P}\ f_{j,P}\ f_{k,P}) = (f_{-j-k,P}) + (f_{j,P}) + (f_{k,P}) = 3(\mathrm{id}) - ((-j-k)P) - (jP) - (kP)$.

32. (Currently Amended) The apparatus as recited in Claim ~~30~~ 27, wherein $f_{-j-k,P}(X)\ f_{j,P}(X)\ f_{k,P}(X)\ \mathrm{line}(jP, kP, (-j-k)P)(X) =$ a constant.

33. (Currently Amended) The apparatus as recited in Claim ~~30~~ 27, wherein if j is an integer and P a point on E, then ~~said~~ the first and second functions are rational functions on E whose divisor of zeros and poles is $(f_{j,P}) = j(P) - (jP) - (j-1)(\mathrm{id})$.

34. (Currently Amended) The apparatus as recited in Claim ~~30~~ 27, wherein ~~said~~ the logic is further configured to determine $f_{0,P}$ such that a line through $0P = \mathrm{id}$, $(-j-k)P$, and $(j+k)P$ is vertical in that it does not reference a y-coordinate.

35. (Original) The apparatus as recited in Claim 34, wherein:

$$f_{j+k,\boldsymbol{P}}(\boldsymbol{X}) = f_{j,\boldsymbol{P}}(\boldsymbol{X}) f_{k,\boldsymbol{P}}(\boldsymbol{X}) \frac{\mathrm{line}\big(j\boldsymbol{P}, k\boldsymbol{P}, (-j-k)\boldsymbol{P}\big)(\boldsymbol{X})}{\mathrm{line}\big(\boldsymbol{id}, (-j-k)\boldsymbol{P}, (j+k)\boldsymbol{P}\big)(\boldsymbol{X})}, \text{ and}$$

$$f_{j-k,\boldsymbol{P}}(\boldsymbol{X}) = \frac{f_{j,\boldsymbol{P}}(\boldsymbol{X})\, line\big(\boldsymbol{id}, j\boldsymbol{P}, -j\boldsymbol{P}\big)(\boldsymbol{X})}{f_{k,\boldsymbol{P}}(\boldsymbol{X})\, line\big(-j\boldsymbol{P}, k\boldsymbol{P}, (j-k)\boldsymbol{P}\big)(\boldsymbol{X})}.$$

36. (Original) The apparatus as recited in Claim 34, wherein:

$f_{j,\mathrm{id}}$ = constant;

$f_{j,-P})(X) = f_{j,P}(-X)$*(constant); and

if ($P + Q + R = \mathrm{id}$), then:

$$f_{j,\boldsymbol{P}}(\boldsymbol{X})f_{j,\boldsymbol{Q}}(\boldsymbol{X})f_{j,\boldsymbol{R}}(\boldsymbol{X}) = \frac{\mathrm{line}(\boldsymbol{P},\boldsymbol{Q},\boldsymbol{R})(\boldsymbol{X})^j}{\mathrm{line}(j\boldsymbol{P},j\boldsymbol{Q},j\boldsymbol{R})(\boldsymbol{X})}.$$

37. (Currently Amended) The apparatus as recited in Claim ~~30~~ 27, wherein P and Q are m-torsion points on E and m is an odd prime, and wherein ~~said~~ the logic is further configured to determine said squared Weil pairing based on

$$\frac{f_{m,\boldsymbol{P}}(\boldsymbol{Q})f_{m,\boldsymbol{Q}}(-\boldsymbol{P})}{f_{m,\boldsymbol{P}}(-\boldsymbol{Q})f_{m,\boldsymbol{Q}}(\boldsymbol{P})} = -e_m(\boldsymbol{P},\boldsymbol{Q})^2,$$

where e_m denotes the Weil-pairing.

38. (Currently Amended) A method comprising:

determining a Squared Weil Pairing $e_m(P, Q)^2$ by:

establishing an odd prime m on a curve E; *and*

based on two m-torsion points P and Q on E, computing $e_m(P, Q)$;

further comprising forming a mathematical chain for m;

wherein for each j in said mathematical chain, a tuple $t_j = [jP, jQ, n_j, d_j]$ is formed such that

$$\frac{n_j}{d_j} = \frac{f_{j,\boldsymbol{P}}(\boldsymbol{Q})f_{j,\boldsymbol{Q}}(-\boldsymbol{P})}{f_{j,\boldsymbol{P}}(-\boldsymbol{Q})f_{j,\boldsymbol{Q}}(\boldsymbol{P})}.$$

39. (Cancelled).

40. (Currently Amended) The method as recited in Claim ~~39~~ 38, wherein said mathematical chain is selected from a group of mathematical chains comprising an addition chain and an addition-subtraction chain.

41. (Currently Amended) The method as recited in Claim ~~39~~ 38, wherein in forming said mathematical chain for m, every element in said mathematical chain is a sum or difference of two earlier elements in said mathematical chain, which continues until m is included in said mathematical chain.

42. (Original) The method as recited in Claim 41, wherein said mathematical chain has a length O(log(m)).

43. (Cancelled).

44. ((Currently Amended) The method as recited in Claim ~~43~~ 38, wherein determining said Squared Weil Pairing further includes:

starting with $t_1 = [P, Q, 1, 1]$, given t_j and t_k, determine t_{j+k} by:

forming elliptic curve sums: $jP + kP = (j+k)P$ and $jQ + kQ = (j+k)Q$;

determining $\text{line}(jP, kP, (-j-k)P)(X) = c0 + c1*x(X) + c2*y(X)$;

determining $\text{line}(jQ, kQ, (-j-k)Q)(X) = c0' + c1'*x(X) + c2'*y(X)$; and

setting

$$n_{j+k} = n_j * n_k * (c0 + c1*x(Q) + c2*y(Q)) * (c0' + c1'*x(P) - c2'*y(P))$$

and

$$d_{j+k} = d_j * d_k * (c0 + c1*x(Q) - c2*y(Q)) * (c0' + c1'*x(P) + c2'*y(P)).$$

45. (Original) The method as recited in Claim 44, further comprising determining t_{j+k} from t_j and t_k, wherein vertical lines through $(j+k)P$ and $(j+k)Q$ do not appear in said formulae for n_{j+k} and d_{j+k} when contributions from Q and $-Q$ are equal, and wherein $-Q$ is the complement of Q and when contributions from P and $-P$ are equal, and wherein $-P$ is the complement of P.

46. (Original) The method as recited in Claim 44, wherein if $j + k = m$, then $n_{j+k} = n_j * n_k$ and $d_{j+k} = d_j * d_k$.

47. (Currently Amended) A computer-readable medium having computer-implementable instructions for causing at least one processing unit to perform acts comprising:

determining a Squared Weil Pairing $e_m(P, Q)^2$ by:

establishing an odd prime m on a curve E; ~~and~~

based on two m-torsion points P and Q on E, computing $e_m(P, Q)^2$;

<u>further comprising forming a mathematical chain for m selected from a group of mathematical chains comprising an addition chain and an addition-subtraction chain, such that every element in the mathematical chain is a sum or difference of two earlier elements in the mathematical chain, which continues until m is included in the mathematical chain;</u>

<u>wherein for each j in the mathematical chain, a tuple $t_j = [jP, jQ, n_j, d_j]$ is formed such that</u>

$$\underline{\frac{n_j}{d_j}=\frac{f_{j,\boldsymbol{P}}(\boldsymbol{Q})f_{j,\boldsymbol{Q}}(\boldsymbol{-P})}{f_{j,\boldsymbol{P}}(\boldsymbol{-Q})f_{j,\boldsymbol{Q}}(\boldsymbol{P})}};$$

<u>outputting validation of mathematical chain and</u>

<u>determining a course of action in response to validation of mathematical chain.</u>

48.-49. (Cancelled).

50. (Currently Amended) An apparatus comprising:

memory configured to store information suitable for use with using a cryptographic process;

<u>a processor</u> logic operatively coupled to ~~said~~ <u>the</u> memory and configured to determine a Squared Weil Pairing $e_m(P, Q)^2$ by establishing an odd prime m on a curve E, and based on two m-torsion points P and Q on E, computing $e_m(P, Q)^2$<u>;</u>

<u>wherein the processor logic is further configured to form a mathematical chain for m that is selected from a group of mathematical chains comprising an addition chain and an addition-subtraction chain;</u>

<u>wherein for each j in the mathematical chain, the logic is further configured to form a tuple $t_j = [jP, jQ, n_j, d_j]$ such that</u>

$$\underline{\frac{n_j}{d_j}=\frac{f_{j,\boldsymbol{P}}(\boldsymbol{Q})f_{j,\boldsymbol{Q}}(\boldsymbol{-P})}{f_{j,\boldsymbol{P}}(\boldsymbol{-Q})f_{j,\boldsymbol{Q}}(\boldsymbol{P})}};$$

<u>a display device coupled to the processor logic for outputting validation of cryptographic process; and</u>

<u>the processor logic determining a course of action in response to cryptographic process.</u>

51.-52. (Cancelled).

53. (Currently Amended) A method comprising:

determining a Squared Weil pairing (m, P, Q), where m is an odd prime number, by setting $t_1 = [P, Q, 1, 1]$, using an addition-subtraction chain to determine $t_m=[mP, mQ, n_m, d_m]$, and if n_m and d_m are nonzero, then determining:

$$\frac{n_m}{d_m} = \frac{f_{m,\boldsymbol{P}}(\boldsymbol{Q})f_{m,\boldsymbol{Q}}(\boldsymbol{-P})}{f_{m,\boldsymbol{P}}(\boldsymbol{-Q})f_{m,\boldsymbol{Q}}(\boldsymbol{P})}; \text{~~and~~}$$

cryptographically processing selected information based on ~~said~~ the Squared Weil pairing by:

generating product identification for selected information;

validating product identification for selected information;

outputting validation of product identification; and

determining a course of action in response to the validation.

54. (Currently Amended) A computer-readable medium having computer-implementable instructions for causing at least one processing unit to perform acts comprising:

determining a Squared Weil pairing (m, P, Q), where m is an odd prime number, by setting $t_1 = [P, Q, 1, 1]$, using an addition-subtraction chain to determine $t_m=[mP, mQ, n_m, d_m]$, and if n_m and d_m are nonzero, then determining:

$$\frac{n_m}{d_m} = \frac{f_{m,\boldsymbol{P}}(\boldsymbol{Q})f_{m,\boldsymbol{Q}}(\boldsymbol{-P})}{f_{m,\boldsymbol{P}}(\boldsymbol{-Q})f_{m,\boldsymbol{Q}}(\boldsymbol{P})}; \text{~~and~~}$$

cryptographically processing selected information based on ~~said~~ the Squared Weil pairing.

using the algorithm to encrypt, decrypt and validate product identification for selected information;

outputting validation of product identification for selected information; and

determining a course of action in response to the validation.

55. (Currently Amended) An apparatus comprising:

memory configured to store information suitable for use with using a cryptographic process;

a processor logic operatively coupled to said memory and configured to:

determine a Squared Weil pairing (m, P, Q), where m is an odd prime number, by setting $t_1 = [P, Q, 1, 1]$,

use an addition-subtraction chain to determine $t_m=[mP, mQ, n_m, d_m]$,

if n_m and d_m are nonzero, then determine

$$\frac{n_m}{d_m} = \frac{f_{m,\boldsymbol{P}}(\boldsymbol{Q})f_{m,\boldsymbol{Q}}(\boldsymbol{-P})}{f_{m,\boldsymbol{P}}(\boldsymbol{-Q})f_{m,\boldsymbol{Q}}(\boldsymbol{P})}; \cancel{\text{and}}$$

cryptographically process selected information based on ~~said~~ the Squared Weil pairing by using the algorithm to encrypt, decrypt and validate selected information;

a display device coupled to the processor for outputting validation of selected information; and

the processor determining a course of action in response to the validation.

56. (Currently Amended) A method comprising:

selecting an elliptic curve;

determining a Squared Tate pairing based on ~~said~~ the elliptic curve,

cryptographically processing selected information based on ~~said~~ the Squared Tate pairing;

wherein m is an odd prime on K and P is an m-torsion point on E, Q is a point on E, with neither P nor Q being the identity and wherein P is not equal to a multiple of Q, and wherein E is defined over K, K has $q = p^n$ elements, and m divides $q-1$, then determining that

$$\left(\frac{f_{m,\boldsymbol{P}}(\boldsymbol{Q})}{f_{m,\boldsymbol{P}}(\boldsymbol{-Q})}\right)^{\frac{q-1}{m}} = v_m(\boldsymbol{P},\boldsymbol{Q}),$$

where v_m denotes the squared Tate-pairing;

outputting validation of selected information; and

determining a course of action in response to validation of selected information.

57. (Original) The method as recited in Claim 56, wherein said elliptic curve includes an elliptic curve E over a field K, wherein E can be represented as an equation $y^2 = x^3 + ax + b$.

58. (Cancelled).

59. (Original) The method as recited in Claim 56, wherein determining said Squared Tate pairing includes determining $v_m(P, Q)$ by:

establishing an odd prime m and said elliptic curve E;

given an m-torsion point P on E and a point Q on E, determining a mathematical chain for m; and

for each j in said mathematical chain, forming a tuple $t_j = [jP, n_j, d_j]$ such that

$$\frac{n_j}{d_j} = \frac{f_{j,\boldsymbol{P}}(\boldsymbol{Q})}{f_{j,\boldsymbol{P}}(\boldsymbol{-Q})}.$$

60. (Original) The method as recited in Claim 59, further comprising:

starting with $t_1 = [P, 1, 1]$, given t_j and t_k, determining t_{j+k} by:

forming an elliptic curve sum $jP + kP = (j+k)P$,

determining $\text{line}(jP, kP, (-j-k)P)(X) = c0 + c1*x(X) + c2*y(X)$, and

setting: $n_{j+k} = n_j * n_k * (c0 + c1*x(Q) + c2*y(Q))$ and

$d_{j+k} = d_j * d_k * (c0 + c1*x(Q) - c2*y(Q))$.

61. (Original) The method as recited in Claim 60 further comprising determining t_{j-k} from t_j and t_k.

62. (Original) The method as recited in Clam 61, wherein if $j+k=m$, then:

$n_{j+k} = n_j * n_k$ and $d_{j+k} = d_j * d_k$.

63. (Original) The method as recited in Claim 61, wherein if n_m and d_m are nonzero, then:

$$\frac{n_m}{d_m} = \frac{f_{m,\boldsymbol{P}}(\boldsymbol{Q})}{f_{m,\boldsymbol{P}}(\boldsymbol{-Q})}.$$

64. (Original) The method as recited in Claim 56, wherein said mathematical chain is selected from a group of mathematical chains comprising an addition chain and an addition-subtraction chain.

65. (Currently Amended) A computer-readable medium having computer-implementable instructions for causing at least one processing unit to perform acts comprising:

determining a Squared Tate pairing based on an elliptic curve; ~~and~~

cryptographically processing selected information based on ~~said~~ the Squared Tate pairing;

wherein m is an odd prime on K and P is an m-torsion point on E, Q is a point on E, with neither P nor Q being the identity and wherein P is not equal to a multiple of Q, and wherein E is defined over K, K has $q = p^n$ elements, and m divides $q-1$, then determining that

$$\left(\frac{f_{m,\boldsymbol{P}}(\boldsymbol{Q})}{f_{m,\boldsymbol{P}}(-\boldsymbol{Q})}\right)^{\frac{q-1}{m}} = v_m(\boldsymbol{P},\boldsymbol{Q}),$$

where v_m denotes the squared Tate-pairing;

outputting validation of selected information; and

identifying a course of action in response to validation of selected information.

66. (Original) The computer-readable medium as recited in Claim 65, wherein said elliptic curve includes an elliptic curve E over a field K, wherein E can be represented as an equation $y^2 = x^3 + ax + b$.

67. (Cancelled).

68. (Original) The computer-readable medium as recited in Claim 65, wherein determining said Squared Tate pairing includes determining $v_m(P, Q)$ by:

establishing an odd prime m and said elliptic curve E;

given an m-torsion point P on E and a point Q on E, determining a mathematical chain for m; and

for each j in said mathematical chain, forming a tuple $t_j = [jP, n_j, d_j]$ such that

$$\frac{n_j}{d_j} = \frac{f_{j,\boldsymbol{P}}(\boldsymbol{Q})}{f_{j,\boldsymbol{P}}(-\boldsymbol{Q})}.$$

69. (Currently Amended) An apparatus comprising:

memory configured to store information suitable for use with using a cryptographic process;

a logic operatively coupled to ~~said~~ the memory and configured to determine a Squared Tate pairing based on an elliptic curve,; and cryptographically processing selected information based on ~~said~~ the Squared Tate pairing;

wherein m is an odd prime on K and P is an m-torsion point on E, Q is a point on E, with neither P nor Q being the identity and wherein P is not equal to a multiple of Q, and wherein E is defined over K, K has $q = p^n$ elements, and m divides $q-1$, then determining that

$$\left(\frac{f_{m,\boldsymbol{P}}(\boldsymbol{Q})}{f_{m,\boldsymbol{P}}(-\boldsymbol{Q})}\right)^{\frac{q-1}{m}} = v_m(\boldsymbol{P}, \boldsymbol{Q}),$$

where v_m denotes the squared Tate-pairing;

a display device coupled to the logic for outputting cryptographic process; and

the logic determining a course of action in response to cryptographic process.

70. (Original) The apparatus as recited in Claim 69, wherein wherein said elliptic curve includes an elliptic curve E over a field K, wherein E can be represented as an equation $y^2 = x^3 + ax + b$.

71. (Cancelled).

72. (Original) The apparatus as recited in Claim 69, wherein said logic is further configured to:

establish an odd prime m and said elliptic curve E;

given an m-torsion point P on E and a point Q on E, determine a mathematical chain for m; and

for each j in said mathematical chain, form a tuple $t_j = [jP, n_j, d_j]$ such that

$$\frac{n_j}{d_j} = \frac{f_{j,\boldsymbol{P}}(\boldsymbol{Q})}{f_{j,\boldsymbol{P}}(\boldsymbol{-Q})}.$$